

Release Notes

FortiSwitchOS 7.2.1



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



August 22, 2022

FortiSwitchOS 7.2.1 Release Notes

11-721-809847-20220822

TABLE OF CONTENTS

Change log	4
Introduction	5
Supported models	5
What's new in FortiSwitchOS 7.2.1	6
Special notices	7
Zero-touch management	7
By default, auto-network is enabled in FortiSwitchOS 7.2.0 and later	7
Downgrading FortiSwitchOS 7.0.0 and later to versions earlier than 6.2.6 or 6.4.4 is not supported	7
Downgrading FortiSwitchOS 7.0.0 and later requires converting the admin password first	7
Connecting multiple FSR-112D-POE switches	8
Upgrade information	9
Product integration and support	10
FortiSwitchOS 7.2.1 support	10
Resolved issues	11
Common vulnerabilities and exposures	11
Known issues	12

Change log

Date	Change Description
June 21, 2022	Initial release for FortiSwitchOS 7.2.1
August 22, 2022	Changed the description of bug 659487.

Introduction

This document provides the following information for FortiSwitchOS 7.2.1 build 0406.

- [Supported models on page 5](#)
- [Special notices on page 7](#)
- [Upgrade information on page 9](#)
- [Product integration and support on page 10](#)
- [Resolved issues on page 11](#)
- [Known issues on page 12](#)

See the [Fortinet Document Library](#) for FortiSwitchOS documentation.

Supported models

FortiSwitchOS 7.2.1 supports the following models:

FortiSwitch 1xx	FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE
FortiSwitch 2xx	FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE
FortiSwitch 4xx	FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FS-M426E-FPOE, FS-448E, FS-448E-POE, FS-448E-FPOE
FortiSwitch 5xx	FS-524D, FS-524D-FPOE, FS-548D, FS-548D-FPOE
FortiSwitch 1xxx	FS-1024D, FS-1024E, FS-1048E, FS-T1024E
FortiSwitch 3xxx	FS-3032E
FortiSwitch Rugged	FSR-112D-POE, FSR-124D

What's new in FortiSwitchOS 7.2.1

Release 7.2.1 provides the following new features:

- VXLAN tunnels are now supported on FS-1024E and FS-T1024E.
- You can now prevent layer-2 loops between virtual tunnel endpoints by having all FortiSwitch units in a VXLAN tunnel act as a single STP root.
- You can now use a routed VLAN interface (RVI) as the VXLAN tunnel initiator or VXLAN tunnel destination.
- You can now configure port-based virtual routing and forwarding (VRF) for an RVI.
- You can now use the dynamic connectivity association key (CAK) mode for Media Access Control security (MACsec).
- You can now use the CLI to change the priority of MAC authentication bypass (MAB) authentication and Extensible Authentication Protocol (EAP) 802.1X authentication.
- Some FortiSwitch models now provide perpetual power over Ethernet (PoE) so that a FortiSwitch unit has uninterrupted power while rebooting.
- You can now configure an automation stitch that will send data to a uniform resource identifier (URI), such as an IP address or URL, when the trigger occurs.
- The new *Router > Multi-Traceroute* page allows you to run multiple path traceroute in the GUI. Results are displayed in a chart and table.
- The *System > FortiLAN Cloud* page now reports the dispatch service, access service, status of SSL verification, and the reason for the last restart.
- The following object identifier (OID) has been added, which refers to a list of FortiSwitch models in the `FORTINET-FORTISWITCH-MIB.mib` file:

Name	OID
sysObjectID	.1.3.6.1.4.1.12356.106.5.SYS_MODEL

Refer to the [FortiSwitch feature matrix](#) for details about the features supported by each FortiSwitch model.

Special notices

Zero-touch management

When a new FortiSwitch unit is started, by default, it will connect to the available manager, which can be a FortiGate device, FortiLAN Cloud, or FortiSwitch Manager. All ports are enabled for auto discovery. The “internal” interface is the DHCP client in all FortiSwitch models. If you do not want your FortiSwitch unit to be managed, you must disable the features that you do not want active.

By default, auto-network is enabled in FortiSwitchOS 7.2.0 and later

After an `execute factoryreset` command is executed on a FortiSwitch unit in standalone mode, the auto-network configuration is enabled by default. If you are not using auto-network, you must manually disable it:

```
config switch auto-network
    set status disable
end
```

Downgrading FortiSwitchOS 7.0.0 and later to versions earlier than 6.2.6 or 6.4.4 is not supported

Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.2.6 and later 6.2 versions is supported. Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.4.4 and later 6.4 versions is supported. Downgrading FortiSwitchOS 7.0.0 to versions earlier than FortiSwitchOS 6.2.6 or 6.4.4 is not supported.

Downgrading FortiSwitchOS 7.0.0 and later requires converting the admin password first

Because FortiSwitchOS 7.0.0 changed from SHA1 to SHA256 encryption for admin passwords, you need to convert the format of the admin password before downgrading from FortiSwitchOS 7.0.0 and later to an earlier FortiSwitchOS version.



If you do not convert the admin password before downgrading from FortiSwitchOS 7.0.0 and later, the admin password will not work after the switch reboots with the earlier FortiSwitchOS version.

The encrypted admin password in FortiSwitchOS 7.0.0 and higher starts with “SH2”, and the encrypted admin password for earlier FortiSwitchOS versions starts with “AK1”.

To convert the format of the admin password in FortiSwitchOS 7.0.0 and later before downgrading to an earlier FortiSwitchOS version:

1. Enter the following CLI command to convert the admin password from SHA256 to SHA1 encryption:

```
execute system admin account-convert <admin_name>
```

2. Downgrade your firmware.

Connecting multiple FSR-112D-POE switches

The FSR-112D-POE switch does not support interconnectivity to other FSR-112D-POE switches using the PoE ports. Fortinet recommends using the SFP ports to interconnect switches.

Upgrade information

FortiSwitchOS 7.2.1 supports upgrading from FortiSwitchOS 3.5.0 and later.

For FortiSwitch units managed by FortiGate units, refer to the [FortiLink Release Notes](#) for upgrade information.

Product integration and support

FortiSwitchOS 7.2.1 support

The following table lists FortiSwitchOS 7.2.1 product integration and support information.

Web browser	<ul style="list-style-type: none">• Mozilla Firefox version 52• Google Chrome version 56 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS (FortiLink Support)	FortiLink is supported on all FortiSwitch models when running FortiOS 5.4.0 and later and FortiSwitchOS 3.2.1 and later.

Resolved issues

The following issues have been fixed in FortiSwitchOS 7.2.1. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
793821	A "Failed to send I2mac trap" message is reported if <code>log-mac-event</code> is enabled on one port without the SNMP-related information being configured.
795444	The performance of the <i>Switch > Monitor > Forwarding Table</i> page needs to be improved.
796655	The <i>Switch > Monitor > 802.1x Status</i> page does not sort the MAC addresses correctly and does not display VLAN traffic.
796779	The <i>Switch > Monitor > IGMP Snooping</i> page does not display IGMP groups.
796806	The <code>set cfg-save revert</code> command under <code>config system global</code> now reboots the FortiSwitch unit after waiting the number of seconds configured in the <code>set cfg-revert-timeout</code> command.
797735	The <code>diagnose sys performance status</code> command should not be available.
798357	When multiple VXLAN configurations use the same remote-ip value, the VXLAN tunnels do not update the underlying SVI IP address.
802529	After rebooting a FortiSwitch unit, IP source guard with DHCP snooping does not work.
802786	Virtual IP addresses cannot be used in a FortiGate device to redirect the public IP address to the private IP address of the FortiSwitch unit.
803112	Customizing the HTTPS port does not work.
803579	The "port24 Overload state. POE disabled" message appears in the log every hour.
807291	After updating the FortiSwitchOS 7.2.0, the switch fails with an "Out of memory: kill process" log message.

Common vulnerabilities and exposures

FortiSwitchOS 7.2.1 is no longer vulnerable to the following CVEs:

- CWE-329

Visit <https://fortiguard.com/psirt> for more information.

Known issues

The following known issues have been identified with FortiSwitchOS 7.2.1. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
382518, 417024, 417073, 417099, 438441	DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANS).
414972	IGMP snooping might not work correctly when used with 802.1x Dynamic VLAN functionality.
480605	<p>When DHCP snooping is enabled on the FSR-112D-POE, the switched virtual interface (SVI) cannot get the IP address from the DHCP server.</p> <p>Workarounds:</p> <ul style="list-style-type: none"> —Use a static IP address in the SVI when DHCP snooping is enabled on that VLAN. —Temporarily disable dhcp-snooping on vlan, issue the <code>execute interface dhcpclient-renew <interface></code> command to renew the IP address. After the SVI gets the IP address from the DHCP server, you can enable DHCP snooping.
510943	<p>The time-domain reflectometer (TDR) function (cable diagnostics feature) reports unexpected values.</p> <p>Workaround: When using the cable diagnostics feature on a port (with the <code>diagnose switch physical-ports cable-diag <physical port name></code> CLI command), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables.</p>
542031	For the 5xx switches, the <code>diagnose switch physical-ports led-flash</code> command flashes only the SFP port LEDs, instead of all the port LEDs.
548783	Some models support setting the mirror destination to “internal.” This is intended only for debugging purposes and might prevent critical protocols from operating on ports being used as mirror sources.
572052	<p>Backup files from FortiSwitchOS 3.x that have 16-character-long passwords fail when restored on FortiSwitchOS 6.x. In FortiSwitchOS 6.x, file backups fail with passwords longer than 15 characters.</p> <p>Workaround: Use passwords with a maximum of 15 characters for FortiSwitchOS 3.x and 6.x.</p>
585550	When packet sampling is enabled on an interface, packets that should be dropped by uRPF will be forwarded.

Bug ID	Description
606044/610149	The results are inaccurate when running cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.
609375	The FortiSwitchOS supports four priority levels (critical, high, medium, and low); however, The SNMP Power Ethernet MIB only supports three levels. To support the MIB, a power priority of medium is returned as low for the PoE MIB.
659487	The FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, and FS-124F-FPOE, FS-148E, and FS-148E-POE models support ACL packet counters but not byte counters. The <code>get switch acl counters</code> commands always show the number of bytes as 0.
667079	For the FSR-112D-POE model: <ul style="list-style-type: none"> If you have enabled IGMP snooping or MLD snooping, the FortiSwitch unit does not support IPv6 functionalities and cannot pass IPv6 protocol packets transparently. If you want to use IGMP snooping or MLD snooping with IPv6 functionalities, you need to enable <code>set flood-unknown-multicast</code> under the <code>config switch global</code> command.
673433	Some 7-meter DAC cables cause traffic loss for the FS- 448E model.
748210	The MAC authentication bypass (MAB) sometimes does not work on the FS-424E when a third-party hub is disconnected and then reconnected.
784585	When a dynamic LACP trunk has formed between switches in an MRP ring, the MRP ring cannot be closed. Deleting the dynamic LACP trunk does not fix this issue. MRP supports only physical ports and static trunks; MRP does not support dynamic LACP trunks. Workaround: Disable MRP and then re-enable MRP.
793145	VXLAN does not work with the following: <ul style="list-style-type: none"> log-mac-event DHCP snooping LLDP-assigned VLANs NAC
795041	The VM debug report (<i>System > Debug Report</i>) is missing information for many CLI commands.



www.fortinet.com

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.